CLAIMS

1. An event-ordering certification method for an event-ordering certification system having a user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, an audit apparatus for auditing authenticity of the certificate and a communication network for connecting the user apparatus, the certification apparatus and the audit apparatus with each other, the method comprising:

an event-ordering request receiving step where the certification apparatus receives the event-ordering request from the user apparatus;

a sequentially assigned data-item calculating step where the certification apparatus drafts a sequentially assigned data-item from the digital information included in the event-ordering request in accordance with a predetermined procedure;

an event-ordering request aggregating step where, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, the certification apparatus calculates assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

a certificate drafting step where the certification apparatus drafts a certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned

thereto;

a certificate sending step where the certification apparatus sends the certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the certificate; and in the complementary information, a complementary information acquirable at a point of assigning the event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

an audit certificate drafting step where after assigning the event-ordering request to the sequential aggregation tree, the certification apparatus assigns a first audit request to the sequential aggregation tree thereby drafting a first audit certificate in the same way as drafting the certificate, acquires a first immediate complementary information for audit at the point of assigning the first audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporates the first immediate complementary information into the first audit certificate;

an audit certificate sending step where the certification apparatus sends the first audit certificate to the audit apparatus;

a complementary information request receiving step where after assigning the first audit request to the sequential aggregation tree, the certification apparatus receives a request of the complementary information of the certificate from the user apparatus;

a late complementary information drafting step where the certification apparatus acquires a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late

complementary information; and

a late complementary information sending step where the certification apparatus sends the late complementary information about the certificate to the user apparatus.

2. The event-ordering certification method of claim 1, wherein at the certificate drafting step, the certification apparatus incorporates the immediate complementary information of the certificate into the first sequential aggregation tree specifying information.

3. The event-ordering certification method of claim 1 or 2, wherein:

the audit certificate drafting step further includes a step where before assigning the event-ordering request to the sequential aggregation tree, the certification apparatus assigns a second audit request to the sequential aggregation tree thereby drafting a second audit certificate in the same way as drafting the certificate, acquires a second immediate complementary information for audit at the point of assigning the second audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporates the second immediate complementary information into the second audit certificate; the event-ordering certification method further comprising:

an audit late complementary information drafting step where after completing the regular time interval, the certification apparatus acquires all of the complementary information about the first and second audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the first and second audit certificates; and

an audit late complementary information sending step where the certification apparatus sends the late complementary information about the first and second audit certificates to the audit apparatus.

4. The event-ordering certification method of any one of claims 1 to 3, wherein at the sequentially assigned data-item calculating step, the sequentially assigned data-item calculated by the certification apparatus comprises a result value obtained by applying a designated collision-resistant hash function on the digital information contained in the event-ordering request.

5. The event-ordering certification method of any one of claims 1 to 4, wherein at the certificate drafting step, the certification apparatus applies a digital signature on the certificate drafted.

6. The event-ordering certification method of any one of claims 1 to 5, further comprising an electronic information publishing step where the certification apparatus electronically publishes the root value of the sequential aggregation tree after completing the regular time interval.

7. The event-ordering certification method of any one of claims 1 to 6, wherein for a plurality of event-ordering requests from the user apparatus, the certificate sending step further includes a step where the certification apparatus sends respective certificates for the event-ordering requests in chronological sequence of assigning the event-ordering requests to the sequential aggregation tree.

8. The event-ordering certification method of claim 2, further comprising, for a plurality of event-ordering requests from the user apparatus:

a sequential aggregation tree storing step where the certification apparatus stores an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as “late complementary

information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

a registration point storing step where the certification apparatus stores an information about the registration points of the plural event-ordering requests, wherein

at the certificate drafting step, the certification apparatus drafts a certificate for the new registration point from the information stored at both of the sequential aggregation tree storing step and the registration point storing step by integrating: the sequential assigned data-item of the new registration point; the first sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto; the immediate complementary information of the new registration point; and the late complementary information of all of the passed registration points of the user apparatus at the new registration point.

9. The event-ordering certification method of claim 2, further comprising, for a plurality of event-ordering requests from the user apparatus:

a sequential aggregation tree storing step where the certification apparatus stores an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

a registration point storing step where the certification apparatus stores an information about an immediately preceding registration point to the new registration point, wherein

at the certificate drafting step, the certification apparatus drafts a certificate for the new registration point from the information stored at both of the sequential aggregation tree storing step and the registration point storing step by integrating: the sequential assigned data-item of the new registration point; the sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto; the immediate complementary information of the new registration point; and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point.

10. The event-ordering certification method of claim 8 or 9, wherein at the sequential aggregation tree storing step, the certification apparatus stores respective positions of nodes in the sequential aggregation tree, which have been subjected to an assignation, and respective assigned values for the nodes, as the information about the sequential aggregation tree.

11. The event-ordering certification method of claim 9, wherein the certification apparatus stores the immediate complementary information of the new registration point and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point, individually in stack.

12. The event-ordering certification method of any one of claims 8 to 11, further comprising an electronic information publishing step where the certification apparatus electronically publishes the root value of the sequential aggregation tree after completing the regular time interval.

13. The event-ordering certification method of any one of claims 8 to 12, further comprising a user's side electronic information publishing step where when the certification apparatus stops an operation thereof or vanishes data

necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the user apparatus electronically publishes both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data.

14. The event-ordering certification method of any one of claims 8 to 13, wherein at the event-ordering request aggregating step after completing the regular time interval, the certification apparatus assigns the root value of the sequential aggregation tree to a leaf of a next sequential aggregation tree so as to form the immediate complementary information about a new registration point assigned to the leaf of the next sequential aggregation tree.

15. An event-ordering certification audit method for an event-ordering certification system having at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, an audit apparatus for auditing authenticity of the certificate and a communication network for connecting the user apparatus, the certification apparatus and the audit apparatus with each other, the method comprising:

an event-ordering request receiving step where the certification apparatus receives a first event-ordering request from the user apparatus;

a sequentially assigned data-item calculating step where the certification apparatus drafts a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

an event-ordering request aggregating step where, in sequential

aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, the certification apparatus calculates assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

a certificate drafting step where the certification apparatus drafts a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

a certificate sending step where the certification apparatus sends the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

an audit certificate drafting step where the certification apparatus assigns a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquires immediate complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree, from the sequential aggregation tree and incorporates the immediate complementary information for audit into the respective audit certificates;

an audit certificate sending step where the certification apparatus sends the audit certificates to the audit apparatus;

a complementary information request receiving step where after sending the first certificate to the user apparatus, the certification apparatus receives a request of the complementary information of the first certificate from the user apparatus;

a late complementary information drafting step where the certification apparatus acquires a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information;

a late complementary information sending step where the certification apparatus sends the late complementary information about the first certificate to the user apparatus;

an audit certificate receiving step where the audit apparatus receives the audit certificates from the certification apparatus;

an audit request receiving step where the audit apparatus receives an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

a first audit certificate selecting step where the audit apparatus selects an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the one audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

a first certificate audit step where the audit apparatus audits validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate

selected at the first audit certificate selecting step coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected at the first audit certificate selecting step; and

an audit result sending step where the audit apparatus sends an audit result of the first certificate to the user apparatus.

16. The event-ordering certification audit method of claim 15, wherein:

the audit certificate receiving step further includes a step of acquiring a first time when the audit apparatus received the audit certificate selected at the first audit certificate selecting step, from a time offering apparatus; and

at the first certificate audit step, the audit apparatus incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result.

17. The event-ordering certification audit method of claim 15 or 16, further comprising

an audit late complementary information drafting step where after completing the regular time interval, the certification apparatus acquires all of the complementary information about the audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the audit certificates;

an audit late complementary information sending step where the certification apparatus sends the late complementary information about the audit certificates to the audit apparatus;

a second audit certificate selecting step where the audit apparatus selects an audit certificate from the audit certificates on a basis of the first sequential

aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

a second certificate audit step where the audit apparatus audits validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected at the second audit certificate selecting step and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected at the second audit certificate selecting step.

18. The event-ordering certification audit method of claim 17, further comprising, for a second event-ordering request from the user apparatus or the other user apparatus, an inter-certificate ordering judgment step where the audit apparatus judges the temporal context between the receipt time of the event-ordering request for the first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates, wherein

at the audit result sending step, the audit apparatus incorporates a chronological sequence in receiving the requests in between the plural certificates into the audit result.

19. The event-ordering certification audit method of claim 17 or 18, further comprising:

a root-value calculating step where the audit apparatus calculates a root

value of the sequential aggregation tree from the plural audit certificates and the late complementary information about the plural audit certificates; and

a root-value validation step where the audit apparatus verifies whether a root value of the sequential aggregation tree published electronically coincides with the root value calculated at the root-value calculating step.

20. The event-ordering certification audit method of any one of claims 17 to 19, further comprising an audit complementary information sending step where the audit apparatus sends the audit certificate selected at the first audit certificate selecting step and the late complementary information about the audit certificate to the user apparatus.

21. The event-ordering certification audit method of any one of claims 17 to 20, wherein:

the audit certificate receiving step further includes a step of acquiring a second time when the audit apparatus sent the audit certificate selected at the second audit certificate selecting step to the user apparatus, from a time offering apparatus; and

at the second certificate audit step, the audit apparatus incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the second time into the audit result.

22. The event-ordering certification audit method of any one of claims 15 to 21, wherein at the first certificate audit step, the audit apparatus applies a digital signature on the audit result.

23. An event-ordering certification apparatus connected to both a user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital

information thereby promoting the event-ordering certification apparatus to draft a certificate and an audit apparatus for auditing authenticity of the certificate through a communication network mutually, for drafting the certificate, for the event-ordering request of the user apparatus, the event-ordering certification apparatus comprising:

event-ordering request receiving means configured to receive the event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the

certificate; and in the complementary information, a complementary information acquirable at a point of assigning the event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured, after assigning the event-ordering request to the sequential aggregation tree, to assign a first audit request to the sequential aggregation tree thereby drafting a first audit certificate in the same way as drafting the certificate, acquire a first immediate complementary information for audit at the point of assigning the first audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporate the first immediate complementary information into the first audit certificate;

audit certificate sending means configured to send the first audit certificate to the audit apparatus;

complementary information request receiving means configured, after assigning the first audit request to the sequential aggregation tree, to receive a request of the complementary information of the certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

complementary information sending means configured to send the late complementary information about the certificate to the user apparatus.

24. The event-ordering certification apparatus of claim 23, wherein the certificate drafting means incorporates the immediate complementary information of the certificate into the first sequential aggregation tree specifying information.

25. The event-ordering certification apparatus of claim 23 or 24, wherein:

the audit certificate drafting means further includes means configured, before assigning the event-ordering request to the sequential aggregation tree, to assign a second audit request to the sequential aggregation tree thereby drafting a second audit certificate in the same way as drafting the certificate, acquire a second immediate complementary information for audit at the point of assigning the second audit request to the sequential aggregation tree from the sequential aggregation tree and incorporate the second immediate complementary information into the second audit certificate; the event-ordering certification apparatus further comprises:

an audit late complementary information drafting means configured, after completing the regular time interval, to acquire all of the complementary information about the first and second audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the first and second audit certificates; and

an audit late complementary information sending means configured to send the late complementary information about the first and second audit certificates to the audit apparatus.

26. The event-ordering certification apparatus of any one of claims 23 to 25, wherein the sequentially assigned data-item calculating means calculates a result value obtained by applying a designated collision-resistant hash function on the digital information contained in the event-ordering request, as the sequentially assigned data-item.

27. The event-ordering certification apparatus of any one of claims 23 to 26, wherein the certificate drafting means applies a digital signature on the certificate drafted.

28. The event-ordering certification apparatus of any one of claims 23 to 27,

further comprising electronic information publishing means configured to publish the root value of the sequential aggregation tree electronically after completing the regular time interval.

29. The event-ordering certification apparatus of any one of claims 23 to 28, wherein for a plurality of event-ordering requests from the user apparatus, the certificate sending means further includes means configured to send respective certificates for the event-ordering requests in chronological sequence of assigning the event-ordering requests to the sequential aggregation tree.

30. The event-ordering certification apparatus of claim 24, further comprising, for a plurality of event-ordering requests from the user apparatus:

sequential aggregation tree storing means configured to store an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about the registration points of the plural event-ordering requests, wherein

the certificate drafting means integrates, from the information stored by both of the sequential aggregation tree storing means and the registration point storing means, the sequential assigned data-item of the new registration point, the first sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto, the immediate complementary information of the new registration point and the late complementary information of all of the

passed registration points of the user apparatus at the new registration point, thereby drafting a certificate for the new registration point.

31. The event-ordering certification apparatus of claim 24, further comprising, for a plurality of event-ordering requests from the user apparatus,

sequential aggregation tree storing step means configured to store an information about the sequential aggregation tree produced at the event-ordering request aggregating means; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about an immediately preceding registration point to the new registration point, wherein

the certificate drafting means integrates, from the information stored by both of the sequential aggregation tree storing means and the registration point storing means, the sequential assigned data-item of the new registration point, the sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto, the immediate complementary information of the new registration point and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point, thereby drafting a certificate for the new registration point.

32. The event-ordering certification apparatus of claim 30 or 31, wherein the sequential aggregation tree storing means stores respective positions of nodes in the sequential aggregation tree, which have been subjected to an assignation, and respective assigned values for the nodes, as the information about the sequential

aggregation tree.

33. The event-ordering certification apparatus of claim 31, wherein the sequential aggregation tree storing means includes a first stack to store the immediate complementary information of the new registration point and a second stack to store the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point.

34. The event-ordering certification apparatus of any one of claims 30 to 33, further comprising electronic information publishing means configured to electronically publish the root value of the sequential aggregation tree after completing the regular time interval.

35. The event-ordering certification apparatus of any one of claims 30 to 34, wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the user apparatus further includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data.

36. The event-ordering certification apparatus of any one of claims 30 to 35, wherein after completing the regular time interval, the event-ordering request aggregating means assigns the root value of the sequential aggregation tree to a leaf of a next sequential aggregation tree so as to form the immediate complementary information about a new registration point assigned to the leaf of the next sequential aggregation tree.

37. An event-ordering certification audit apparatus connected to both at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information and a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, through a communication network, for auditing authenticity of the certificate, wherein the certification apparatus comprises:

event-ordering request receiving means configured to receive a first event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first

event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured to assign a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquire immediate complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree from the sequential aggregation tree and incorporate the immediate complementary information for audit into the respective audit certificates;

audit certificate sending means configured to send the audit certificates to the audit apparatus;

complementary information request receiving means configured, after sending the first certificate to the user apparatus, to receive a request of the complementary information of the first certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

late complementary information sending means configured to send the late complementary information about the first certificate to the user apparatus, and

wherein the event-ordering certification audit apparatus comprises:

audit certificate receiving means configured to receive the audit

certificates from the certification apparatus;

audit request receiving means configured to receive an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

first audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

first certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate selected by the first audit certificate selecting means coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, also configured to further certify a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the first audit certificate selecting means; and

audit result sending means configured to send an audit result of the first certificate to the user apparatus.

38. The event-ordering certification audit apparatus of claim 37, wherein:

the audit certificate receiving means further includes means configured to acquire a first time when the audit apparatus received the audit certificate selected by the first audit certificate selecting means, from a time offering apparatus; and

the first certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result.

39. The event-ordering certification audit apparatus of claim 37 or 38, wherein

the certification apparatus further comprises:

audit late complementary information drafting means configured to acquire all of the complementary information about the audit certificates drafted by the audit certificate drafting means from the sequential aggregation tree after completing the regular time interval, thereby forming a late complementary information about the audit certificates; and

audit late complementary information sending means configured to send the late complementary information about the audit certificates to the audit apparatus, and

wherein the event-ordering certification audit apparatus further comprises:

second audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

second certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected by the second audit certificate selecting means and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the second audit certificate selecting means.

40. The event-ordering certification audit apparatus of claim 39, further comprising, for a second event-ordering request from the user apparatus or the other user apparatus, inter-certificate ordering judgment means configured to judge the temporal context between the receipt time of the event-ordering request for the

first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates, wherein

the audit result sending means incorporates a chronological sequence in receiving the requests in between the plural certificates into the audit result.

41. The event-ordering certification audit apparatus of claim 39 or 40, further comprising:

root-value calculating means configured to calculate a root value of the sequential aggregation tree from the plural audit certificates and the late complementary information about the plural audit certificates; and

root-value validation means configured to verify whether a root value of the sequential aggregation tree published electronically coincides with the root value calculated at the root-value calculating step.

42. The event-ordering certification audit apparatus of any one of claims 39 to 41, further comprising audit complementary information sending means configured to send the audit certificate selected by the first audit certificate selecting means and the late complementary information about the audit certificate to the user apparatus.

43. The event-ordering certification audit apparatus of any one of claims 39 to 42, wherein:

the audit certificate receiving means further includes means configured to acquire a second time when the event-ordering certification audit apparatus sent the audit certificate selected by the second audit certificate selecting means to the user apparatus, from a time offering apparatus; and

the second certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first

certificate is temporally ahead of the second time into the audit result.

44. The event-ordering certification audit apparatus of any one of claims 39 to 42, wherein the first certificate audit means applies a digital signature on the audit result.

45. An event-ordering certification program for allowing the certification apparatus to perform the respective steps of the event-ordering certification method of any one of claims 1 to 14.

46. An event-ordering certification audit program for allowing the certification apparatus to perform the respective steps of the event-ordering certification audit method of any one of claims 15 to 22.

47. A program for validation of event-ordering certificates for a user apparatus in an event-ordering certification audit system where at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus and an audit apparatus for auditing authenticity of the certificate are connected with each other through a communication network,

wherein the certification apparatus comprises:

event-ordering request receiving means configured to receive a first event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a

directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured to assign a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquire immediate complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree from the sequential aggregation tree and incorporate the immediate complementary information for audit into the respective audit certificates;

audit certificate sending means configured to send the audit certificates to the audit apparatus;

complementary information request receiving means configured, after

sending the first certificate to the user apparatus, to receive a request of the complementary information of the first certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

late complementary information sending means configured to send the late complementary information about the first certificate to the user apparatus, and

wherein the audit apparatus comprises:

audit certificate receiving means configured to receive the audit certificates from the certification apparatus;

audit request receiving means configured to receive an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

first audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

first certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate selected by the first audit certificate selecting means coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, also configured to further certify a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt

time of the audit request for the audit certificate selected by the first audit certificate selecting means; and

audit result sending means configured to send an audit result of the first certificate to the user apparatus, and

wherein the event-ordering certification program allows the user apparatus to perform:

an event-ordering request sending step of sending the first event-ordering request to the certification apparatus;

a certificate receiving step of receiving first event-ordering request from the certification apparatus

a complementary information request sending step of sending the request of the complementary information of the first certificate to the certification apparatus;

a complementary information receiving step of receiving the complementary information of the first certificate from the certification apparatus;

an audit request sending step of sending the audit request to the audit apparatus; and

an audit result receiving step of receiving the audit result for the first certificate.

48. The program for validation of event-ordering certificates of claim 47, wherein:

the audit certificate receiving means further includes means configured to acquire a first time when the audit apparatus received the audit certificate selected by the second audit certificate selecting means from a time offering apparatus; and

the first certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result, and

wherein the program for validation of event-ordering certificates allows the user apparatus to perform an event-ordering request drafting step of acquiring a

third time at the point of sending the first event-ordering request to the certification apparatus from the time offering apparatus and incorporating a value as a result of calculating the third time in accordance with a designated procedure into the first event-ordering request.

49. The program for validation of event-ordering certificates of claim 47 or 48, wherein the certification apparatus further comprises:

audit late complementary information drafting means configured to acquire all of the complementary information about the audit certificates drafted by the audit certificate drafting means from the sequential aggregation tree after completing the regular time interval, thereby forming a late complementary information about the audit certificates; and

audit late complementary information sending means configured to send the late complementary information about the audit certificates to the audit apparatus, and

wherein the audit apparatus further comprises:

second audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

second certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected by the second audit certificate selecting means and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the second audit certificate

selecting means.

50. The program for validation of event-ordering certificates of claim 49, wherein:

the audit apparatus includes, for a second event-ordering request from the user apparatus or the other user apparatus, inter-certificate ordering judgment means configured to judge the temporal context between the receipt time of the event-ordering request for the first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates;

the audit result sending means incorporates a chronological sequence in receiving the requests in between the first and second certificates into the audit result; and

the audit request for the first certificate includes a request for judging its chronological sequence in relation to the second certificate.

51. The program for validation of event-ordering certificates of claim 49, wherein:

the audit apparatus includes audit complementary information sending means configured to send the audit certificate selected by the first audit certificate selecting means and the late complementary information about the audit certificate to the user apparatus; and

the program for validation of event-ordering certificates allows the user apparatus to perform a step of receiving the audit certificate and its late complementary information sent from the audit apparatus.

52. The program for validation of event-ordering certificates of any one of claims 48 to 51, wherein:

the audit certificate receiving means further includes means configured to acquire a second time when the event-ordering certification audit apparatus sent the audit certificate selected by the second audit certificate selecting means to the user apparatus, from a time offering apparatus;

the second certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the second time into the audit result; and

the program for validation of event-ordering certificates allows the user apparatus to perform an event-ordering request drafting step of acquiring a third time at the point of sending the first event-ordering request to the certification apparatus from the time offering apparatus and incorporating a value as a result of calculating the third time in accordance with a designated procedure into the first event-ordering request.

53. The program for validation of event-ordering certificates of any one of claims 47 to 52, wherein the program for validation of event-ordering certificates allows the user apparatus to perform:

a root-value calculating step of calculating a root value of the sequential aggregation tree from the first certificate sent from the certification apparatus and all of the late complementary information about the first certificate acquired after completing the regular time interval; and

a root-value validation step of verifying whether a root value for the sequential aggregation tree published electronically after completing the regular time interval coincides with the root value calculated at the root-value calculating step.

54. A program for validation of event-ordering certificates for allowing a computer to verify authenticity of certificates, the computer being connected to first and second user apparatuses, each of which performs an event-ordering request for certifying a chronological sequence of a certain event in time-series

events generating a designated digital information, and an event-ordering certification apparatus for drafting the certificates for a plurality of event-ordering requests of the first and second user apparatuses through a communication network,

wherein the event-ordering certification apparatus comprises:

event-ordering request receiving means configured to receive the event-ordering requests from the first and second user apparatuses;

sequentially assigned data-item calculating means configured to draft sequentially assigned data-items from digital information included in the event-ordering requests in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

sequential aggregation tree storing means configured to store an information about the sequential aggregation trees produced by the event-ordering request aggregating means;

assuming that: a leaf of the sequential aggregation tree to which the sequentially-assigned data-item drafted from each of the event-ordering requests is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the registration point; in the complementary information, a complementary information acquirable at a point of assigning each of the sequentially assigned data-item to the sequential aggregation

tree is defined as an immediate complementary information, while a complementary information acquirable after the point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as a late complementary information; the late complementary information of a leaf a1 determined at a point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about the registration points of the event-ordering requests with respect to each of the user apparatuses;

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information of all past registration points of each of the user apparatuses, thereby drafting a certificate for the new registration point; and

certificate sending means configured to send the certificates to the user apparatuses;

wherein each of the user apparatuses comprises:

event-ordering request sending means configured to send the event-ordering requests to the event-ordering certification apparatus;

certificate receiving means configured to receive the certificates for the event-ordering requests from the event-ordering certification apparatus;

certificate storing means configured to store the certificates received;

validation request sending means configured to send a certificate for validation to the computer; and

validation result receiving means configured to receive a validation result of the certificate for validation from the computer;

wherein the program for validation of event-ordering certificates allows the computer to perform:

a certificate receiving step of receiving two certificates for validation from the first and second user apparatuses respectively or two certificates for validation from the first user apparatus;

assuming that one of the two certificates judged as being temporally former in publishing order is a first certificate, while the other of the two certificates judged as being temporally latter in publishing order is a second certificate, based on the sequential aggregation tree specifying information of the two certificates received,

a sequential aggregation tree specifying information sending step of sending the sequential aggregation tree specifying information in the second certificate to the user apparatus receiving the first certificate;

a late complementary information receiving step of receiving the late complementary information about the first certificate at a registration point after publishing the second certificate, from the user apparatus receiving the first certificate;

a validation step of verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the second certificate coincides with an assigned value for the specified node calculated from the first certificate and the late complementary information or not, thereby certifying validity of the first and second certificates and that the registration point of the first certificate is temporally ahead of the registration point of the second certificate, based on a validation result; and

a validation result sending step of sending the validation result to both or either of the first and second user apparatuses.

55. The program for validation of event-ordering certificates of claim 54,

wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval,

each of the user apparatuses includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data, and

when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the program for validation of event-ordering certificates allows the computer to perform a "by user's side publishing value" validation step of verifying that both received data at the certificate receiving step and received data at the late complementary information receiving step are not tampered by judging whether each assigned value for the one or more nodes published by the user apparatus through the user's side electronic information publishing means coincides with an assigned value calculated by both the received data at the certificate receiving step and the received data at the late complementary information receiving step.

56. A program for validation of event-ordering certificates for allowing a computer to verify authenticity of certificates, the computer being connected to first and second user apparatuses, each of which performs an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, and an event-ordering certification apparatus for drafting the certificates for a plurality of event-ordering requests of the first and second user apparatuses through a communication network,

wherein the event-ordering certification apparatus comprises:

event-ordering request receiving means configured to receive the event-ordering requests from the first and second user apparatuses;

sequentially assigned data-item calculating means configured to draft sequentially assigned data-items from digital information included in the event-ordering requests in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

sequential aggregation tree storing means configured to store an information about the sequential aggregation trees produced by the event-ordering request aggregating means;

assuming that: a leaf of the sequential aggregation tree to which the sequentially-assigned data-item drafted from each of the event-ordering requests is assigned is defined as a registration point; an information about other nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the registration point; in the complementary information, a complementary information acquirable at a point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as an immediate complementary information, while a complementary information acquirable after the point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as a late complementary information; the late complementary information of a leaf a1 determined at a point of completing an assignation for a leaf a2 on the right of the

leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about an immediately preceding registration point with respect to each of the user apparatuses;

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information about the immediately preceding registration point of each of the user apparatuses at the new registration point, thereby drafting a certificate for the new registration point; and

certificate sending means configured to send the certificates to the user apparatuses;

defining that a rightmost registration point of the respective registration points of each of the user apparatuses is referred to as a provisional terminal point and that to calculate all of the complementary information about a designated registration point acquirable at a point of completing an assignment for the provisional terminal point is referred to as an incremental completion for a certificate of the designated registration point,

wherein each of the user apparatuses comprises:

event-ordering request sending means configured to send the event-ordering requests to the event-ordering certification apparatus;

certificate receiving means configured to receive the certificates for the event-ordering requests from the event-ordering certification apparatus;

certificate storing means configured to store the certificates received;

incremental completion means configured to perform the incremental completion to a certificate for validation of the plural certificates received and stored;

validation request sending means configured to send a certificate for validation to the computer; and

validation result receiving means configured to receive a validation result of the certificate for validation from the computer;

wherein the program for validation of event-ordering certificates allows the computer to perform:

a certificate receiving step of receiving two certificates for validation from the first and second user apparatuses respectively or two certificates for validation from the first user apparatus;

assuming that one of the two certificates judged as being temporally former in publishing order is a first certificate, while the other of the two certificates judged as being temporally latter in publishing order is a second certificate, based on the sequential aggregation tree specifying information of the two certificates received,

a sequential aggregation tree specifying information sending step of sending the sequential aggregation tree specifying information in the second certificate to the user apparatus receiving the first certificate;

a late complementary information receiving step of receiving the late complementary information about the first certificate at a registration point after publishing the second certificate, from the user apparatus receiving the first certificate;

a validation step of verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the second certificate coincides with an assigned value for the specified node calculated from the first certificate and the late complementary information or not, thereby certifying validity of the first and second certificates and that the registration point of the first certificate is temporally ahead of the registration point

of the second certificate, based on a validation result; and

a validation result sending step of sending the validation result to both or either of the first and second user apparatuses.

57. The program for validation of event-ordering certificates of claim 56, wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval,

each of the user apparatuses includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data, and

when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the program for validation of event-ordering certificates allows the computer to perform a "by user's side publishing value" validation step of verifying that both received data at the certificate receiving step and received data at the late complementary information receiving step are not tampered by judging whether each assigned value for the one or more nodes published by the user apparatus through the user's side electronic information publishing means coincides with an assigned value calculated by both the received data at the certificate receiving step and the received data at the late complementary information receiving step.

58. The program for validation of event-ordering certificates of claim 47, wherein the certification apparatus further comprising, for a plurality of event-ordering requests from the user apparatus:

sequential aggregation tree storing means configured to store an

information about the sequential aggregation tree produced by the event-ordering request aggregating means;

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about the immediately preceding registration point,

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information about the immediately preceding registration point of each of the user apparatuses at the new registration point, thereby drafting a certificate for the new registration point; and

certificate sending means configured to send the certificates to the user apparatuses; and

defining that a rightmost registration point of the respective registration points of each of the user apparatuses is referred to as a provisional terminal point and that to calculate all of the complementary information about a designated registration point acquirable at a point of completing an assignment for the provisional terminal point is referred to as an incremental completion for a certificate of the designated registration point, wherein the program for validation of event-ordering certificates allows the computer to perform:

an event-ordering request sending step of sending the event-ordering requests to the certification apparatus;

a certificate receiving step of receiving the certificates for the event-ordering requests from the certification apparatus;

a certificate storing step of storing the certificates received; and

an incremental completion step of performing the incremental completion to a certificate for validation of the plural certificates received and stored.

59. The program for validation of event-ordering certificates of any one of claims 56 to 58, wherein the incremental completion is carried out with the use of the certificates that the user apparatus received from the certification apparatus and further stored therein and without forming a tree structure.

60. The program for validation of event-ordering certificates of claim 59, wherein for respective elements forming the complementary information about a designated registration point acquirable at a point of completing an assignment for the provisional terminal point, the incremental completion is carried out by firstly selecting one certificate out of one or more certificates that the user apparatus received from the certification apparatus and further stored therein, the one certificate containing either the elements directly or information enough to calculate the elements, and secondly calculating the elements from the one certificate selected.

61. The program for validation of event-ordering certificates of claim 59, wherein the complementary information is carried out to all of registration points positioned on the left of the provisional terminal point of the user apparatus.

62. The program for validation of event-ordering certificates of claim 61, defining that, for one registration point a1 of the user apparatus on the left of the provisional terminal point and another registration point a2 of the user apparatus closest to the point a1 on a left side thereof, to calculate all of the complementary information about the registration point a2 acquirable at a point of completing an

assignment of the provisional point from all of the complementary information about the registration point a1 acquirable at the point of completing the assignment of the provisional point and receipts at the registration points a1 and a2, is referred to as a propagation procedure for completion, wherein

the incremental completion is carried out without forming a tree structure by the steps of:

originating in calculating or acquiring all of the complementary information about a registration point a of the user apparatus, which information is acquirable at a point of completing the assignment of the provisional terminal point, from the certificate that the user apparatus received and stored, the registration point a being closest to the provisional terminal point on a left side thereof;

starting a calculating process of all of the complementary information about respective registration points on the left of the provisional terminal point, which information is acquirable at a point of completing an assignment of the provisional terminal point, from a rightmost registration point a of the registration points; and

applying the calculating process on the registration points on the left of the registration point a in sequence while using the propagation procedure for completion.

63. The program for validation of event-ordering certificates of any one of claims 56 to 62, wherein the incremental completion is accomplished by a method comprising the steps of:

extracting respective registration points up to the provisional terminal point appropriately;

dividing into local areas each between the registration points extracted;

performing an incremental completion on the assumption that a rightmost assigned registration point in each of the local areas is a provisional terminal point; and

calculating all of acquirable complementary information about the extracted registration points.

64. The program for validation of event-ordering certificates of any one of claims 56 to 63, wherein

the certification apparatus has electronic information publishing means configured to publish the root value of the sequential aggregation tree electronically after completing the regular time interval; and

the program for validation of event-ordering certificates allows the user apparatus to perform:

a root-value calculating step of calculating a root value of the sequential aggregation tree from an information about the designated registration point and the complementary information calculated at the incremental completion step after completing the regular time interval; and

a root-value validation step of verifying whether the root value published electronically coincides with the root value calculated.

65. An event-time validation program readable by a computer that verifies a time when the user apparatus executing the program for validation of event-ordering certificates of claim 48 or 52 applies on the event-ordering request, wherein the event-time validation program allows the computer to perform:

an audit result acquiring step of acquiring the audit result;

an event-ordering request acquiring step of acquiring the event-ordering request corresponding to the audit result;

a time validation step of judging validity of the third time on a basis of a time difference between the third time and at least either the first time or the second time; and

a step of outputting the judgment.